Estimation and analysis of wireless sensor network parameters through neural network: A Special Investigation on Malicious Activities

SYNOPSIS

SUBMITTED
TO
IIMTUNIVERSITY, MEERUT
PARTIAL FULLFILMENT OF THE
REQUIREMENT FOR THE AWARD OF
DOCTOR OF PHILOSOPHY

SESSION 2022-23

SUPERVISOR:
Dr. Suraj Malik

SCHOLAR:
Ms. Aruna Kumari
Ph.D- Scholar

IIMT UNIVERSITY, GANGA NAGAR MEERUT

1. WSN Introduction

A new technology that has drawn considerable attention from scientists is Wireless Sensor Networks (WSN). Generally, the WSN environment needs low power, low overhead, and a large number of sensors that are randomly distributed at the target position or manually redeployed. Wireless sensor nodes are underpowered in terms of networking, computing, and energy. The transmitted message is an efficient and common wireless sensor network prototype that enables several users to quickly combine and relay packets of messages.

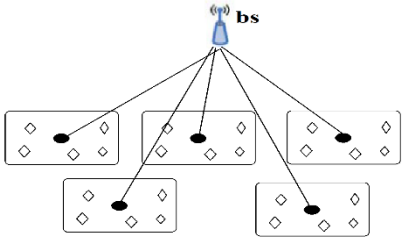

Figure 1.1: WSN presenting Clustering formation

In a range of systems, wireless sensor networks are used, including mapping, surveillance, environmental reconnaissance, and weather forecasting for civil and military applications. There is inadequate storage capacity in the node battery for this type of network, so it is very important to utilize the resources in the WSN nodes efficiently and appropriately to improve the life of the network.These sensor nodes are known as compact lightweight devices capable of interacting, sensing and analyzing data across a larger network than one node to the target node. They have a narrow contact range and therefore send the information directly to the desired consumer with the distribution of the transmission spectrum. Most commonly, because of their meagre means, they do not have the capacity to withstand a strong attacker. By making use of active IDS, it is possible to classify attackers who have planned huge attack techniques. Unfortunately, most sensor networks are quite sensitive to attacks due to the characteristics of WSN, and opponents may simply produce network traffic, and may even trigger substantial packet drops when transmitting the packet or changing the original material. For the packet to propagate. Authentication mechanisms are implemented on the network to ensure secure contact between nodes. Secure transmission of data between nodes within WSN networks is important.

The electronic network architecture needs strong standards for data transmission from one end to the other. This can be done only by a cellular network, since the internet era now uses encrypted contact. As a transmission mechanism, an open wireless channel environment is used between the source and destination nodes. This wireless connectivity is categorized by Wireless Sensor Networks (WSN) and Wireless Body Field Networks (BFN) over (WBAN). WBAN is used in humans and it senses body conditions in multiple parts of the human body and transmits this information to the remote computer. The sensor numbers are propagated randomly in the case of WSNs and information is collected from all the sensors. This sensed information is sent to the remote computer as a receiver. The number of sensors clustered together in a node is shown by the block head. The block header receives all the physical information from its clustered nodes and this information is transmitted to a distant watershed by each community chief.

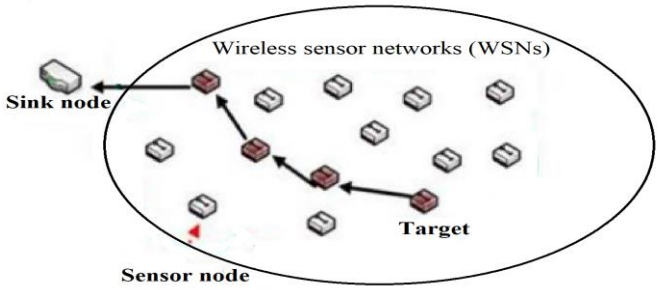

Figure 1.2: Nodes deployment in WSN network

A number of community headers can be reached on WSN networks with a single node in the basin. A sensor, an analog-to-digital converter, and a processor are all included with each WSN. The sensor senses the surrounding parameters in analogue mode and uses an analog-to-digital converter to transform this analogue sensor data into digital data. This transformed digital data is processed via a processor machine and this processed data is transmitted to another node via a built-in wired antenna attached to the node. Figure 1.2 displays the sensor nodes built in the WSN environment along with the basin nodes connected with the networks of the WSN. The activity of the nodes is changed by remote attackers or intruders and these nodes become malicious/stealth. The efficiency of current WSNs' performance is decreased by the number of malicious/hidden nodes. Therefore, in order to increase performance, this paper suggests an important solution to WSN node discovery.

A network of wireless sensors is a form of wireless network comprising a wide number of devices called sensor nodes (called nodes). Circular, robotic, micro power and low-power systems are such devices. These networks, of course, cover a broad variety of distributed and battery-powered networked handheld computers for data collection, aggregation, and operator distribution, and have perfected skills in computation and processing. Nodes are small computers that shape a network by working together.

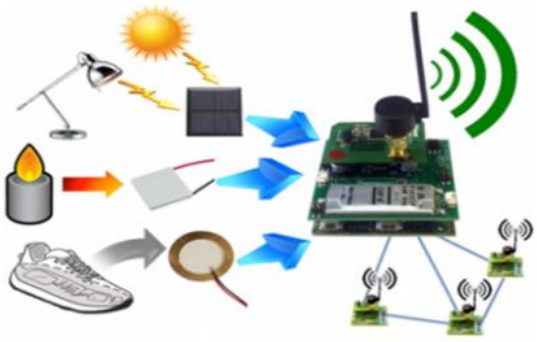

Figure 1.3: wireless sensor network

The sensor node is a wireless system that is energy-efficient and multifunctional. Industrial food applications are common. To fulfil clear application aims, the sensor node assembly gathers data from the surrounding regions. The dying can use transmitters and receivers to communicate with one another. The death toll on a wireless sensor network could be in the hundreds or even thousands. Ad hoc networks have few nodes and no architecture, unlike network sensors.

2. Review of Literature

Sunitha&Chandrika, (2016),The Industrial Internet of Things (IIoT) has attracted great attention from academia and industry with the growth of information technologies and smart manufacturing. With diverse implementations in many areas, including environmental tracking, Wireless Sensor Networks (WSN) have many benefits, making them a very significant part of the Internet of Things. Power exhaustion and hardware failures, however, in WSNs will cause node

failure. Wireless channel transmission may even be influenced by the manufacturing climate, contributing to network stability challenges, even with closely integrated data and control levels in conventional networks, which also raises the expense and difficulty of network management. Uh. Com. They are adding a new Software Information Network (SDN) in this document and changing this network to propose a system named the Wireless Sensor Network (SD-WSN) Improved Software Specified. The following issues may be solved through this new structure.

1) Address the issue of network optimization and smooth convergence of WSN into IoT for large-scale heterogeneous networks.

2) The issue of network coverage is overcome, which increases the network's stability.

3) Due to different issues, particularly related to power consumption, the system handles node failure. The stability of wireless sensor networks must also be enhanced by designing complex schemes to minimize power consumption and latency time for network nodes under IoT conditions. Experiments have shown that node power usage and delay time are greatly decreased by the enhanced solution, thereby improving WSN efficiency.

Barki et al. (2018),In MANET networks, the complex behavior of the nodes renders administration and management challenging. Researchers also worked to develop the routing protocol used in order to address these issues. In this paper, from a compilation of methods and techniques suggested by researchers in this area, they investigate the impact of ANN in the assessment of quality and efficiency in MANET networks and try to use this analysis in a summary table to conclude conclusions and potential improvements to these methods.

Singh & Dhaka (2016),Dynamic conditions that shift fast over time are tracked by wireless sensor networks. This complex behavior is triggered by external variables or is initiated by the programmers of the device themselves. Sensor networks also implement deep learning approaches to remove the need for excessive overhaul in order to respond to those conditions. Machine learning often inspires several realistic ideas that optimize the usage of energy and prolong the network's existence. In this paper, they offer a systematic overview of the 2002-2014 literature of machine learning approaches used in Wireless Sensor Networks (WSN) to solve popular problems. The benefits and drawbacks of each suggested algorithm are measured against the corresponding problem. In order to help WSN programmers build machine learning strategies tailored to their application problems, they also have a comparative reference. They give an outline of applications for embedded networks and address the criteria that arise from this discussion. In addition, inside the network, they speak about selected processing strategies and mention the similarity between neural and posterior Hopfield propagation networks. It is described within the sense of the sensor network in the following neural networks. In the framework of sensor networks, they define the motivation and operational condition of neural networks and they analyses the first findings obtained from their implementation of the test. With these models, they claim, there is a high potential that promises a strong influence on future study, especially when implemented as hybrid technology. In order to locate a Packet Loss in the sensor network, they are doing this for WNS and also to try to find out the throughput importance of data sent via the sensor network.

Gupta & Pal (2016),Wireless ad hoc networks map complex conditions that shift quickly over time. This complex behavior is triggered by external variables or is initiated by the programmers of the device themselves. Ad hoc networks also

implement machine learning methods in order to respond to certain situations to eliminate the need for needless overhaul. Machine learning often inspires several realistic ideas that optimize the usage of energy and prolong the network's existence. In this paper, they present a detailed literature analysis of machine learning approaches that have been used to resolve popular issues in ad hoc wireless networks (WSN) between 2002-2014. The benefits and drawbacks of each suggested algorithm are calculated against the corresponding problem. In order to help WSN programmers build machine learning strategies tailored to their application problems, they also have a comparative reference. They give an outline of applications for embedded networks and address the criteria that arise from this discussion. In addition, inside the network, they speak about selected processing strategies and mention the similarity between neural and posterior Hopfield propagation networks. It is discussed within the context of the ad hoc network in the following neural networks. In the framework of ad hoc networks, they define the motivation and operational condition of neural networks and analyses the first findings obtained from the application of experiments. With these models, they claim, there is a high potential that promises a strong influence on future study, especially when implemented as hybrid technology. They enforce this such that in an ad hoc network, WNS detects a Packet Loss and they often aim to figure out the throughput benefit of data sent through the ad hoc network. On ad hoc wireless networks, they simulate a Trojan attack and determine the network impact. Using MATLAB-10 simulation programmer, they conduct their simulations consisting of a list of all network protocols to model different current network architectures. MATLAB-10 does not include any malicious protocol emulation units, but it includes dedicated wireless routing protocols. Therefore, they first apply a new Trojan protocol to MATLAB-10, to simulate Trojan assaults. In order to simulate a Trojan threat, they began their research by writing a new AODV protocol using MAT files. They conducted experiments on multiple topologies to assess network output with and without Trojans on the network after adding a new routing protocol that simulates a Trojan horse. Unsurprisingly, network efficiency has dramatically degraded due to the existence of Trojans. Next, to remove the impact of the Trojan horse on the AODV network, they suggested an IDS approach. In MATLAB-10, they apply the solution. And they test the conclusions as they did with the Trojan. As a consequence, their approach, with a 24-38 percent success rate, removed the Trojan influence.

Vij&Joon (2017),Wireless sensor networks consist of individual nodes that, by the identification or regulation of physical parameters, may communicate with the world. For the success of their assignments, these nodes shall collaborate. The nodes are interconnected and each Wireless Sensor Network (WSN) is a community of sensors with limited resources capable of interacting and collaborating with each other to accomplish a shared objective by wireless connexions. In rugged conditions, such as battlefields and observation zones, sensor nodes run. They give an outline of applications for embedded networks and address the criteria that arise from this discussion. In addition, inside the network, they speak about selected processing strategies and mention the similarity between neural and posterior Hopfield propagation networks. It is described within the sense of the sensor network in the following neural networks. In the framework of sensor networks, they define the motivation and operational condition of neural networks and they analyses the first findings obtained from their implementation of the test. With these models, they claim, there is a high potential that promises a strong influence on future study, especially when implemented as hybrid technology. In order to locate a Packet Loss in the sensor network, they are doing this for WNS and also to try to find out the throughput importance of data sent via the sensor network. On the MATLAB command prompt and the Interface produced during the quest, another complete simulation was performed. Find great value for all words for parcel delivery, such as efficiency, E2Edaly, and PDR. The propagation of the neural network with a large PARAM value will then offer a safer option for

spontaneous WSN Packet Loss Detection tests and prevent more packet drops. They discovered it by checking the GUI seven times before and seven times for recommendation, based on recommended studies. It is obvious that only 51 packets were missing when the 1280 packet delivery was sent and 105 packets were lost earlier when sending the same data packet. So, they have a rather noticeable outcome of the suggested work in digital records. Compared to before, almost twice. So, it is very obvious that when a neural network with high PARAM value is implemented, thanks to highly active pattern recognition technologies, it has a great improvement in reducing packet loss to a minimal, which would also correct the loss concern. From packets. Therefore, both the final delay and output changed marginally. The suggested systems therefore do a better job of identifying accidents during transmission and stopping them.

Zhao et al. (2018),The target tracking problem has always been the wireless sensor network access point, and with the introduction of a modern streaming and multimedia streaming application, new streaming efficiency criteria have been proposed to drive target tracking; Thus, in this paper , they propose a network-based software-defined adaptive hierarchical routing algorithm for a wireless sensor The algorithm takes both network strength and efficiency into account, uses the Hopfield Neural Network algorithm to determine the optimal path as local routing (LR) between neighboring clusters, and adopts a local route-based multiple-choice backpack problem model. For the end to be reached. -- Worldwide final instructions, under various objective scenarios, to obtain target monitoring knowledge routing. Physical trials and simulated studies are used in the test bed. The experimental findings indicate that, in various test conditions, the suggested algorithm is superior to the Low Energy Adaptive Cluster Hierarchy (LEACH) and the Sequential Mapping Directive.

Alhashemi&Almomani (2019),Current advances in the field of communication are contributing to ongoing and immediate demands for innovative technology in the field of data transmission that can render the communication process more efficient and stable. Recently, WSN has arisen as a common and significant form of network that can be utilized in a setting that a human being cannot continuously handle. In order to drive the efficiency of WSN in terms of different parameters, including age and capacity, it is possible to use different behavior, such as meeting. As a common grouping strategy in WSN, KSOM appeared. The purpose of this article is to determine WSN's efficiency in terms of average life and energy consumed after introducing Kohen to the role of the neural network. Results revealed that compared to the LEACH procedure, lifetime efficiency improved by 9.1 percent, while energy usage decreased by 3.03 percent.

Ahad et al. (2016),Due to the highly complex and frequently uncertain environmental factors that define wireless networks, modern wireless network architecture, including decision making and parameter optimization, is incredibly challenging. In order to cope with this dynamic architecture, there is a common trend in digital networks to integrate artificial intelligence (AI) technologies. The well-established Artificial Intelligence Architecture for Neural Networks (NN), which is well recognized for its extraordinary generality and flexibility, has been adopted, although a range of AI innovations have been profitably utilized in the wireless networking community. For cellular networks in a number of settings. In particular, for tasks that require sorting, learning, or development, NNs are particularly common. They include a presentation of common NN models in this paper, as well as a detailed analysis of NN applications in wireless networks. In specific, as they evaluate alternate AI frameworks and technologies, they also discuss the drawbacks and complexities of NN implementation. While there are several NN surveys in the literature, to their knowledge, their paper is the first in red based on NN applications in wireless networks.

Alarifi&Tolba (2019),The wireless sensor network (WSN) architecture is enabled by the Cloud Aided Internet of Things (C-IoT). The sensor network for Internet of Things (IoT) sensor nodes is a self-contained collection of independent resource constraints. In a dedicated way, the nodes connect to transfer knowledge across the simulated world from the server. WSN clustering aims to increase the efficiency of the network by regulating the use of resources and improving the precision of data processing. The C-IoT service prices are increased through this. It needs complicated clustering algorithms to optimize IoT sensor networks via power and overhead control. The required output enhancement during streaming in a virtualized setting may not be accomplished by a simple stacking scheme. This document aims to suggest, with the assistance of the sensor network, an augmentation-based learning system, Adaptive Q-Learning (AQL), to enhance network efficiency with minimal power-offset in CIoT. AQL functions in two separate phases: selecting the party chief and choosing the carrier. In order to rate a contract based on its previous actions through the show, a decision-making mechanism is used. Using the conditions of adaptive redirection and head placement, AQL optimizes coordination with and within classes. The simulation results show the accuracy of the proposed AQL by retaining, considering the decreased overhead on the sensor network, the number of active nodes in the network and its constant power. The efficiency of CIoT is significantly enhanced with the realization of constructive characteristics in sensor networks. Experimental findings indicate that the proposed learning technology is successful in enhancing network existence with a strong demand response rate and reducing waits, higher prices, and request failures.

Madhav (2017), In the analysis, a data compression method using Huffman code, LEACH and Dijkstra algorithms showing effective nodes of data transmission maximized the useful life of the network. A major security concern arises during transmission, primarily in military areas or other high security areas where several attackers attempt to break records. The research performed on network protection is therefore aimed at establishing a security pattern to secure the data transmitted over the network. Noise, redundancy, and missing values are some of the other typical problems arising on the network during packet transmission. The completed work given an adaptive preprocessing approach that uses Principal Component Analysis (PCA) and the Hopfield Hyperbolic Neural Network (HHNN) to streamline data flow in order to solve these problems. By increasing the precision of the forecast, this method gives greater performance. Collecting and scheduling data in various aquarium settings is the other major issue with WSN. The study used TDMA scheduling to predict delays in data collection and reduce high power usage in order to solve the issue, whereas the pocket route algorithm (PDT) decreases redundancy. The findings indicate that in the simulation, the quest was successful. The results of the simulation show high performance in terms of reduced delays, increased network existence, increased security, decreased power usage, and decreased data loss during wireless sensor network data transmission. The suggested study has now been effectively conducted, producing stronger performance than other existing approaches used to address some of the issues handled by wireless sensor networks.

Dang et al. (2020),The internal fingerprint position technique based on channel status information (CSI) has received widespread interest. However, due to low fingerprint resolution, unsatisfactory classification and matching effect, and sensitivity to environmental effects, this approach struggled to have a stronger locating effect and a higher locating accuracy. This article proposes a CSI-driven internal fingerprint position mechanism based on the Hopfield Discrete Neural Network (DHNN) to solve the problem. The strategy generally consists of offline and online steps. A low-pass filter is used to preprocess the fingerprint information for each reference point in the offline stage, after which the step difference is followed to correct the fingerprint details of all the reference points. This increases the accuracy of fingerprint data, while eliminating issues such as internal environmental shifts, the impact of multi-path signals, etc.

impacting fingerprint data. Finally, after collecting reasonably detailed fingerprint details, a premium fingerprint database was developed. Data from each landmark in the fingerprint database is allocated as attractors in the online process, to ensure data accuracy. Meanwhile, for affinity decision through DHNN, the position information of the test point is processed. Ultimately, they find the results of the translation. The experimental findings have shown that localization accuracy with an average error of 1.6 m can be accomplished in the experimental setting using the proposed procedure. It has better stability compared with alternative approaches, and can significantly minimize labor costs and time.

Dang et al. (2020),The internal fingerprint position technique based on channel status information (CSI) has received widespread interest. However, due to low fingerprint resolution, unsatisfactory classification and matching effect, and sensitivity to environmental effects, this approach struggled to have a stronger locating effect and a higher locating accuracy. This article proposes a CSI-driven internal fingerprint position mechanism based on the Hopfield Discrete Neural Network (DHNN) to solve the problem. The strategy generally consists of offline and online steps. A low-pass filter is used to preprocess the fingerprint information for each reference point in the offline stage, after which the step difference is followed to correct the fingerprint details of all the reference points. This increases the accuracy of fingerprint data, while eliminating issues such as internal environmental shifts, the impact of multi-path signals, etc. impacting fingerprint data. Finally, after collecting reasonably detailed fingerprint details, a premium fingerprint database was developed. Data from each landmark in the fingerprint database is allocated as attractors in the online process, to ensure data accuracy. Meanwhile, for affinity decision through DHNN, the position information of the test point is processed. Ultimately, they get the results of the translation. The experimental findings have shown that localization accuracy with an average error of 1.6 m can be accomplished in the experimental setting using the proposed procedure. It has better stability compared with alternative approaches, and can significantly minimize labor costs and time.

Jyoti, (2016),A Wireless Sensor Network (WSN) is made up of a large number of sensor nodes that are constrained in the spectrum of battery power and connectivity and have different models of sensor capability. Environmental tracking is one of the most significant features of a wireless sensor network. A Wireless Sensor Network (WSN) incorporates autonomous, spatially dispersed sensors to monitor physical or maintenance requirements such as noise, sound, vibration, temperature, motion, or pollutants and to collaboratively transmit their data across the network to a key location (base station or basin). Only multi-directional antennas are fitted with wireless sensor networks, which may cause heavy Packet Losss. In these networks, the output per node tends to decline as the number of nodes grows. To minimize interruption, it is also recommended to transmit with several short-range hops. The clash of packets allows wireless networks to destroy packets and consume energy. Thanks to explosive flow and pollution across the ports, it gets worst in thick WSNs. To retrieve the found beams, they suggest a neural network diagram in this paper. The proposed study prevents Packet Loss with a neural network in Hopfield and improves the pace of packet transmission and network latency, thus reducing the delay of end2.

Din et al. (2020),The usage of sensors has been in high demand in all systems, as well as in today's lives. The public domain has also begun to shift towards smartphone apps that are more available. For eg, school child monitoring, fitness tracking, tracking device, fire detection, etc. Therefore, the preferred alternative for satisfying these needs is a Wireless Sensor Network (WSN). However, WSN itself remains hindered by restricted battery use notwithstanding the

excitement for developing different applications with the sensors. Various forms of studies have been undertaken to resolve this concern owing to certain applications that need a long battery life. The role of artificial intelligence (AI) to improve the sensor's battery life is one of those reasons. Fuzzy Reasoning (FL) is one of the favored AI structures that researchers have opted to incorporate for WSN to improve WSN's lifetime in particular. There are three organic functions of Fuzzy Logic that must be tested for potential in WSN applications. To achieve the best results for studying the usage of sensor batteries, the recommended solution is to mix various forms of fuzzy logic organic functions that are triangle with Gaussian and Gaussian with trapezoid and trapezoid with triangle. Touch cost, core strength, and residual power as mist input are criteria used for community head selection. This solution would use an established multilevel algorithm (Plot) algorithm and this is part of the development of the MAP towards WSN's lifetime. During data transmission, the findings can compare, examine and analyses the dead node count and power use of the sensor node. In conclusion, the lifetime of the sensor network will be increased with this approach since the technology introduced can reduce the energy consumption of sensor nodes.

Li &Serpen (2016),This article suggests that an artificial neural network be used in a completely distributed parallel computing mode in a wireless sensor network. The aim is to provide cognitive knowledge and adaptability for the wireless sensor network for better autonomous activity. A case study in which a Hopfield neural network designed as a static optimizer for a poorly linked dominant group problem is used in a wireless sensor network to enable it to tailor the network architecture to future improvements immediately and after deployment in the field illustrates the applicability and usefulness of the proposed model. In order to reflect the network infrastructure, the loosely related minimum dominance range established for the wireless sensor network topology diagram model is used and can be recalculated any time the topology of the sensor network shifts. A simulation analysis was performed with up to 1000 TOSSIM emulators utilizing the TinyOS-Mica sensor network platform. The time complexity, message complexity, and consistency indicators of the approach to the case study were measured and assessed. The simulation results showed that, as a static optimizer, the WSN integrated with the Hopfield neural network was competing with other local or distributed algorithms to demonstrate its viability for the poorly related dominant group query.

Karthikeyan et al. (2017),In order to find the shortest stuck path, numerous intellectual enhancement demonstrations, such as artificial neural networks (ANN), genetic algorithms (GA), etc., have been scheduled. As the two major fields are dedicated cell networks (MANET) and wireless sensor networks (WSN), rapid expansions of wireless connectivity have been accomplished largely in the sector of mobile phone networks. In the mobile wireless network, fabric avoidance is the greatest obstacle, i.e., the topology of the network varies with time owing to energy conservation or node versatility. The dilemma of dynamic optimization is related to the versatility of the nodes in order to find the shortest path (SP) in this network. The nodes normally die or may switch due to power reduction, and this situation makes it more challenging for the network to find the shortest path. In this paper, they propose a new approach for the identification and orientation of shorter dynamic paths in MANET using genetic algorithms (GA). One of the fastest rising wireless networks of the next decade is MANETs. Initial findings show that after each update, the GA-based algorithm will respond rapidly to environmental change (i.e. change in network topology) and generate high-quality solutions.

Polastre et al. (2004),They include an in-depth analysis of the use of wireless sensor (WSN) networks to track real-world ecosystems. To meet the requirements of biologists, a series of system design requirements covering node hardware

design, sensor network software, protective enclosures, and system layout have been created. 43 nodes were installed on a tiny island off the coast of Maine in the summer of 2002 to relay valuable data live on the site. While researchers expect that certain difficulties would emerge in the application of WSN in the modern world, several challenges can only be found by practice. They offer a portfolio of four months of deployment experience on a remote island. To test device performance, they analyses environmental data and node health. The WSN's close integration with its climate offers environmental evidence at historically unimaginable densities. They illustrate that sensor knowledge is often helpful in forecasting device efficiency and network faults. They evaluate node and network architecture on the basis of more than 1 million data readings and build network reliability profiles and models of failure.

Robinson et al. (2019),In this article, they suggest a new Wireless Sensor Network (WSN) energy-conscious routing protocol focused on threshold rate and fuzzy logic to increase energy performance. The heads of the groups are picked on the basis of the WSN likelihood values for each node, which are derived from each node's residual energy. To measure the average strength of the whole network at the current level, the cumulative residual energy of the node is used. The nodes are more likely to have a greater probability of being chosen as the block head, which receives packets over a single hop link from the block member. Using blurry power of multi-hop coordination, the head of the block forwards the gathered data to the drain. Three parameters are used for fuzzy control: the duration of the tail of the node, the size of the node from the base station, and the residual power of the node. Data from tests suggests that by complementing certain methods, the proposed energy effective cluster routing protocol system (called MLSEEP) achieves stronger results than current protocols.

Venu&Rahman (2019),Without any center or administrative nodes, an ad hoc cell network briefly sets up the network. Generally speaking, to relay data or messages, AODV can find the fastest path from the foundation to the end point. An on-demand custom vector protocol (RPFAODV) focused on restricted flood prediction is included in their proposed solution. The objective of RPFAODV is on defining the endpoint node, predicting the path based on the power level of each node, the position of the end node through the route request packet, and the route answer packet messages. Once a path answer packet has been sent from an end node to a source node, it is now configured to transfer the data packet to the destination as a party. The unnecessary node crossing in this suggested protocol is constrained by the prediction of the network route. In the other transmitting field of the network they forward the data or notification from the destination to the local coverage nodes. Better output outcomes compared to other traditional routing protocols In this paper, in addition to the interactive AODV protocols, the RPFAODV protocol was analyzed and its individuality was measured with appreciation for the numerous movements centered on the speed of message transmission, the end-to - end latency, amount of dropped packets, and Network Simulator (NS2) throughput.

Shakeel et al. (2021), presented a WSNs are often employed in a wide range of monitoring applications, including healthcare, environmental, and systemic health surveillance, in addition to military surveillance. Reducing network resource utilisation is critical for programmes that are often put in places that are difficult for people to access. Most WSN protocols have been developed to help expand the network's presence. The results from this research, which utilised a Hopfield neural network, are organised next to one other so as to facilitate comparison. This study also describes how to manage WSN collisions quickly and correctly. Future studies that include neural networks and a significant amount of fuzzy logic will help to avoid these problems in the future.

Kaur& Sharma (2020), presented a WSN technologies are highly approached, since they previously had to

communicate with at least a few sensor nodes from several applications. Sensor node power consumption affects the WSN, since the application monitoring node depends on collected data from the sensor node. The amount of energy used to transfer packets throughout the whole network, the percentage of packets that get dropped along the way, the number of packets that get sent to the base station and cluster head are all considered factors. Dead nodes (which have a one-in-a-few (or more) chances of surviving each round) are also obtained via the simulation.

Rao et al. (2020), presented the intrusion detection technique that is presented in this study is an entirely new approach that takes into consideration network trust and sensor packet loss rate. The suggested approach finds rogue nodes by digging deep into packet loss. For packet loss rate assessment, two independent metrics such as buffer capacity metric and residual energy metre are used. Another thing the trust assessment takes into consideration is fundamental sensor-node communication. An experiment is performed using the suggested methodology and its effectiveness is gauged by FPR and MDR (MDR). The findings suggest that the recommended strategy has superior outcomes.

Lodhi&Sattar (2019), presented a WSNs, also known as wireless sensor networks (WSNs), consist of autonomous nodes located in discrete locations (often outdoors) and connected to sensors to sense and maintain physical and environmental conditions. In practise, however, these protocols slow down the cluster head and hence reduce the rate at which packets are processed. By using this statistic, they show how to identify the "optimal ability to control packet loss" and how to prolong the network lifespan. This measure gives an indication of the energy and memory state of nodes. The knapsack method is used to calculate the residual status of an intermediate node. NS2 conducts an evaluation of our suggested work, and the findings reveal that our protocol works better than previous protocols.

Jaradat et al (2019), presented an application for real-world deployment of the LEACH protocol is given in this research study, in which a simulation model is presented for use in evaluating the protocol's performance in a noisy WSN (wireless sensor network) environment. This model represents the noise level as the probability of packet receipt (pr). When the number of peers on the network is less than one, the network is regarded to be noise-free and all packets transmitted are received. The suggested simulation model was constructed using Python, a computer language that offers more support for simulation development. The homogeneous LEACH algorithm's performance was evaluated for multiple network metrics in the presence of varied noise levels. A noise-free, analytically determined energy model was developed.

Rahmadhani et al. (2018), presented a LEACH (Low Energy Adaptive Clustering Hierarchy) which is a wireless sensor network clustering routing system (WSN). The setup and steady state phases of the LEACH algorithm are separated. LEACH Routing has a significant packet loss on a busy network. They need a Delay Tolerant Network to tackle the issue (DTN). DTN is a sophisticated design that enables communication under difficult situations, such as a congested network. LEACH-WSN and LEACH-WSN over DTN show no significant differences in terms of energy consumption in two scenarios, but when they look at the lifespan of nodes, which is dependent on energy consumption, LEACH-WSN over DTN has an early death node. When the number of nodes grows or the network becomes congested, LEACH-WSN has a major advantage over DTN.

Mugheri et al. (2018), presented a WSN, security has always been a primary issue. WSN currently lacks a robust security solution for its operations because to limited resources and node size constraints. Some of the purposed security approaches for WSN are evaluated in this study for concerns that still remain in the purposed security techniques. Some of the documented or implemented security algorithms by researchers are being researched to do the analysis on security approaches, and the flaws with such algorithms are being identified. Following the study, it is evident that the majority of the algorithms being developed by academics for WSN must be constructed with WSN's resource constraints in mind.

Vhatkar et al. (2017), presented the wireless sensor network (WSN) has emerged as a popular kind of network, particularly in environments where human interaction is an issue. In a WSN, a group of sensors in a sensing environment work together to monitor and regulate the physical properties of an environment. WSN needs an energy efficient routing protocol to effectively complete the specified job while maintaining a longer network lifespan. In this study, the performance of two hierarchical routing protocols, ECHERP (Equalized Cluster Head Election Routing Protocol) and PDCH (PEGASIS with Double Cluster Head), is examined using different QoS criteria such as delay, throughput, packet drop ratio, and energy usage.

Tedeschi et al. (2017), presented a Node's misbehaving may cause packet losses. Malicious nodes and network assaults may both lead to packet losses. It is vital that a clear understanding of the reason be included into effective response methods in order to get the network up and running again. They validated their model using sensor data and discovered that our model accurately represents the packet loss causes. As a result, they were able to find the most precise and granular factors for packet loss.

Thrimoorthy et al. (2017),They must have a network connection in order to exchange data across several devices. The devices may be any electronic equipment that works with data transfer protocols, such as computers, laptops, smartphones, or sensors that are connected to a router through wireless or cable connections. Wired and wireless networks are both examples of network-networks. They study sensors as network devices in the article which has been provided. Whenever there is congestion, there are a host of unintended effects, such delayed decisions, packet loss, higher network overhead when retransmitting lost packets, and lower sensor life spans. In this research, a virtual model is offered that may aid in comprehending how data are exchanged through a network of sink nodes and sensors, as well as a mechanism for detecting and controlling congestion.

Khan et al. (2013), introduced the Low latency and consistent message transmission is a benefit of wireless sensor networks (WSNs) in mission-critical and delay-sensitive industrial applications. Reliable communication between the sink and the sensing nodes is vital in applications like gas leakage detection, monitoring of pressure, and control of industrial processes. Nodes are deployed densely in varied contexts with no specified network architecture in wireless sensor networks. Also, this article discusses three potential network topological configurations that might support mission-critical applications. They used three distinct topological designs known as Linear, Tier-1, and Split Tier-1 to analyse the performance of a wireless sensor network (WSN).

Liu et al. (2014),examined the delay performance in a wireless sensor network (WSN) using a cluster-tree topology in this research. Due to the close relationship between sensors and sinks, as well as the resource allocations of cluster heads, end-to-end latency might be greatly reliant on how widely distributed the sensors are in relation to the sinks (CHs). The results of this experiment help to establish the packet loss rate. After proposing a heuristic to jointly discover the timeline allocations of all the CHs in a WSN in order to achieve the minimal and balanced packet drop rate for traffic originating from different levels of the cluster tree, a proposed heuristic for a balance between latency and packet drop rate is then introduced. Simulation results are used to illustrate that the suggested CH timeframe allocation strategy is effective and also to validate the study. Accordingly, the system life sensor hub relies upon the battery life. For this situation, viable information driven WSN is a standard test as a unique test. Therefore, any improvement in these networks should focus on improving the energy consumption of the network. Unfortunately, malicious node can cause rapid eradication of energy during the attacker node. This is why the most important investigation work is to look for the fall energy analysis due to the worst node.

2.1 Research Gap

The review study of this WSN found that the detection of suspicious activities research has less for WSN infrastructure

through some intelligent mechanism. The prior studies like flexible synthesis, Support Vector Machine usually use to detect the malicious nodes and attacks. The most of the venerable to attack situation supposed to be in the WSN as par the general findings of the reviews. The review study of this WSN found that the detection of suspicious activities research has less for WSN infrastructure through some intelligent mechanism. The prior studies like flexible synthesis, Support Vector Machine usually use to detect the malicious nodes and attacks. The most of the venerable to attack situation supposed to be in the WSN as par the general findings of the reviews.

2.2 Problem Statement

It is quite hard to detect the suspicious activities in WSN communication. As considering the hues node implanted in the area, the detection of suspicious activities in WSN also going to very difficult. It is quite hard to detect the suspicious activities in WSN communication. As considering the hues node implanted in the area, the detection of suspicious activities in WSN also going to very difficult.

3. **Objectives of the work**

- To study the different parameters of WSN.
- To study the malicious activities of WSN.
- To estimate the parametric loss of WSN communication
- Compare the parametric loss of WSN communication in different topologies.
- Improvise the techniques to detect the malicious activities of WSN.

4. Proposed Methodology

This research has main focus of detection of Malicious Nodes in WSN. For this we are considering the Neural Networks as the mechanism to perform the random creation of test and differentiate the time domain activities. The machine learning like Neural network must has very good tools to monitoring the WSN. The sudden various of change of activities in pattern of the network could be monitored through the proposed neural network. The delay and the loss of communication packet in the proposed network is the key findings of this research. For this we have to apply the neural network to Improvise the techniques to detect the malicious activities of WSN.

5. Tools

- MATLAB
- SPSS/A-MoS

Reference

1. Narayana, V. L., &Midhunchakkaravarthy, D. (2020, July). A Time Interval based Blockchain Model for Detection of Malicious Nodes in MANET Using Network Block Monitoring Node. In *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)* (pp. 852-857). IEEE.

2. Gao, B., Amagata, D., Maekawa, T., & Hara, T. (2020). Detecting Energy Depriving Malicious Nodes by Unsupervised Learning in Energy Harvesting Cooperative Wireless Sensor Networks. *Journal of Information Processing*, *28*, 689-698.

3. Jaint, B., Indu, S., Pandey, N., &Pahwa, K. (2019, October). Malicious Node Detection in Wireless Sensor Networks Using Support Vector Machine. In *2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)* (pp. 247-252). IEEE.

4. Zhang, W., Zhu, S., Tang, J., &Xiong, N. (2018). A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks. *The Journal of Supercomputing*, *74*(4), 1779-1801.

5. Jamshidi, M., Darwesh, A. M., Lorenc, A., Ranjbari, M., &Meybodi, M. R. (2018). A precise algorithm for detecting malicious sybil nodes in mobile wireless sensor networks. *IEIE Transactions on Smart Processing & Computing*, *7*(6), 457-466.

6. Shakeel, N., Haroon, M., & Ahmad, F. (2021). A Study of WSN and Analysis of Packet Drop During Transmission. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*.

7. Kaur, K., & Sharma, E. S. (2020). Analysis Grid Based DEEC Protocol with Priority Queue for Increasing Lifetime Of WSN. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *7*(2), 699-703.

8. Rao, A. N., Naik, B. R., Devi, L. N., &Subbareddy, K. V. (2020, September). Trust and Packet Loss Aware Routing (TPLAR) for Intrusion Detection in WSNs. In *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 386-391). IEEE.

9. Lodhi, A. K., &Sattar, S. A. (2019). Cluster Head Selection by Optimized Ability to Restrict Packet Drop in Wireless Sensor Networks. In *Soft Computing in Data Analytics* (pp. 453-461). Springer, Singapore.

10. Jaradat, Y., Masoud, M., Jannoud, I., Abu-Sharar, T., &Zerek, A. (2019, March). Performance analysis of homogeneous LEACH protocol in realistic noisy WSN. In *2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)* (pp. 590-594). IEEE.

11. Rahmadhani, M. A., Yovita, L. V., &Mayasari, R. (2018, July). Energy consumption and packet loss analysis of LEACH routing protocol on WSN over DTN. In *2018 4th International Conference on Wireless and Telematics (ICWT)* (pp. 1-5). IEEE.

12. Mugheri, A. A., Siddiqui, M. A., &Khoso, M. (2018). Analysis on Security Methods of Wireless Sensor Network (WSN). *Sukkur IBA Journal of Computing and Mathematical Sciences*, *2*(1), 52-60.

13. Vhatkar, S., Shaikh, S., &Atique, M. (2017, February). Performance analysis of equalized and double cluster head selection method in wireless sensor network. In *2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-5). IEEE.

14. Tedeschi, A., Midi, D., Benedetto, F., &Bertino, E. (2017). Statistically-enhancing the diagnosis of packet losses in WSNs. *International Journal of Mobile Network Design and Innovation*, *7*(1), 3-14.

15. Thrimoorthy, N., Anuradha, T., & Kumar, A. (2017, September). A virtual model to analyze congestion in a wireless sensor network (WSN). In *2017 International Conference on Advances in Electrical Technology for Green Energy (ICAETGT)* (pp. 28-32). IEEE.

16. Khan, M. F., Felemban, E. A., Qaisar, S., & Ali, S. (2013, December). Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs). In *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks* (pp. 324-329). IEEE.

17. Liu, W., Zhao, D., & Zhu, G. (2014). End-to-end delay and packet drop rate performance for a wireless sensor network with a cluster-tree topology. *Wireless Communications and Mobile Computing*, *14*(7), 729-744.